UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 1:23-cr-86

v.

Hon. Hala Y. Jarbou

TAYSEER YOUSEF,

Defendant.
_____/

OPINION

The Government has charged Defendant Tayseer Yousef with conspiracy to transport stolen goods interstate (count one), and interstate transportation of stolen goods (counts two and three). The stolen goods at issue are cell phones. He asks the Court to suppress evidence seized by the Government from the execution of two separate search warrants, one for an iCloud account and one for his residence. (Def.'s Mot. to Suppress, ECF No. 30.) Defendant contends that the affidavits submitted to obtain the warrants were facially insufficient to support probable cause. The Court will deny his motion.

I. BACKGROUND

A. Warrant for iCloud Account

On June 29, 2021, a special agent for the Department of Homeland Security Investigations ("HSI") requested a warrant to search an iCloud account associated with a phone number ending in 1166. According to the warrant affidavit (iCloud Warrant Aff., ECF No. 36-1), HSI had worked with the Kent County Sheriff's Office in Michigan ("KCSO") to investigate a string of burglaries in West Michigan, many of which involved the theft of cell phones that were being sold to a source in Chicago, Illinois.

For instance, on June 6, 2020, a KCSO detective arrested an individual while he was attempting to rob a car dealership in Kent County. (*Id.* at 4.) At the time, the individual was on bond for two burglaries of cell phone stores. Police identified the individual as a member of a gang called 1K Chicken Boys. Two days later, police obtained a warrant to search the robber's phone. Through that search, police discovered a text message dated June 1, 2020, in which the robber asked another member of 1K Chicken Boys to "send the plug number." (*Id.* at 5.) According to the agent, "'Plug' is a term used to describe a dealer or hook up, meaning someone able to provide cash for stolen items[.]" (*Id.*) In a response text, the other gang member identified the 1166 number as the plug. Police also discovered an outgoing Facetime communication from the robber's cell phone to the 1166 number on June 5, 2020. The robber had identified the number as "Chi Plug" in their phone's address book. (*Id.*)

In July 2020, police spoke with a suspect in custody regarding the burglary of a cell phone store in Fremont, Michigan. (*Id.*) The suspect told police that members of 1K Chicken Boys were taking stolen cell phones to Chicago and selling them to a subject known as "Habibi" or "Arab." (*Id.* at 6.) When reviewing Facebook records of the suspected robbers and/or gang members (including members of 1K Chicken Boys), police discovered four requests for the phone number of "Arab" or the "plug" in May 2020, to which respondents provided the 1166 number. (*Id.* at 5-7.)

In December 2020, police arrested an individual for a bond violation and obtained a warrant to search his cell phone. The search revealed several texts between the individual and the 1166 number discussing the sale of phones. (*Id.* at 9.)

Through a "TLO database" search, police discovered that the 1166 number is associated with Defendant Tayseer Yousef, residing in Oak Forest, Illinois. (*Id.*) Additional records searches

revealed that there was a 2014 Toyota Avalon registered in Defendant's name. (*Id.* at 10.) And the agent learned through his own database searches that Defendant had used the 1166 number when communicating with immigration authorities in January 2021. (*Id.* at 12.)

Through further investigation, police discovered that an iPhone stolen from a T-Mobile store on January 20, 2021, was registered to an individual named Anna Yousef in Chicago on January 22, 2021. (*Id.*) A TLO search indicated that the individual had a "relative connection" to Defendant, though the "familial relationship" was unclear. (*Id.*) Similarly, another iPhone stolen during that same robbery was registered on January 21, 2021, to Joanna Yousef, who also lived in Chicago. (*Id.* at 13.) Joanna and Anna were associated with the same address in the TLO database. (*Id.*)

On February 12, 2021, police discovered that Defendant's vehicle had been recorded passing by a license plate reader in New Buffalo, Michigan, on November 15 and 23, 2020, December 6, 2020, and January 20, 2021. (*Id.* at 10-11.) Those dates correspond to the dates of robberies of various cell phone stores in Kent County and Coldwater, Michigan. (*Id.* at 10-11.)

That same month, police obtained and searched the phone of a suspect involved in the theft of cell phones from an AT&T store in Grand Rapids, Michigan, on December 29, 2020. (*Id.* at 16-19.) In the iCloud data for that phone, police discovered communications with the 1166 number about the stolen phones. For instance, around the time of the robbery, the suspect asked the 1166 number for a "price list"; the 1166 number responded with prices for three different models of the iPhone 12. (*Id.* at 19.) The suspect responded that he possessed AT&T versions of iPhones and then sent two photos to the 1166 number. (*Id.* at 19-20.) One photo showed multiple cell phones, many of which were still in their packaging. The other photo showed the unique identification

number of a phone on the back of its packaging. (*Id.* at 20.) That identification number matched one of the phones stolen from the AT&T store. (*Id.*)

The agent also explained how he knew that the 1166 number belonged to an iPhone:

> iCloud account contents typically only capture cell phone conversations when both participants are using an iPhone and have the iMessages feature enabled . . . . [T]he conversation between [the robbery suspect] and [the 1166 phone] was obtained in the iCloud backup data for the iCloud account associated with [the robbery suspect], indicating that the phone using [the 1166 number] is an Apple iPhone.

(*Id.* at 24.)

On March 11, 2021, police obtained a picture of a "male subject" sitting in the driver's seat of what appears to be a Toyota Avalon. (*Id.* at 11.) In the photograph, the subject is sitting next to a stack of cell phones. The agent asserted that the "side facial portion" of the driver in the photograph is "consistent with" the Illinois driver's license photograph for Defendant. (*Id.*)

In April 2021, police obtained a warrant for the location information of the phone using the 1166 number. On the morning of May 11, 2021, robbers stole 30 cell phones from a store in Walker, Michigan. Later that day, location information for the phone using the 1166 number showed that it traveled from Chicago to just across the state line in Indiana, and then returned to Chicago. (*Id.* at 15-16.)

B. Warrant for Defendant's Residence

In November 2021, an HSI agent requested a warrant to search Defendant's apartment in Tinley Park, Illinois. (Residence Warrant Aff., ECF No. 26-3.) The warrant affidavit included much of the above investigation history regarding Defendant and the 1166 number, including: (1) references to the 1166 number as a "plug" in a text message by a member of 1K Chicken Boys and in the address book of a phone seized by the police; (2) a suspect's statement to police that an individual in Chicago called "Habibi" and "Arab" purchased stolen cell phones from members of 1K Chicken Boys; (3) messages by members of 1K Chicken Boys referring to the 1166 number as

belonging to "Arab"; (4) the TLO database search tying Defendant to the 1166 number and to a 2014 Toyota Avalon; (5) Defendant's use of the 1166 number when communicating with immigration authorities; (6) records from the license plate reader about the presence of the Toyota Avalon in Michigan on the dates of five different robberies involving cell phones; (7) the photograph of an individual in the driver's seat of a Toyota vehicle, sitting next to a stack of cell phones, whose side facial profile was consistent with Defendant's; and (8) the registration of two stolen cell phones by people believed to be family members of Defendant.

In addition, on February 3, 2021, police located a stolen vehicle used during an unsuccessful cell phone store robbery in Jenison, Michigan. (*Id.* at 14.) The driver of the vehicle possessed two cell phones. A search of the cell phones revealed text messages and calls from the 1166 number.

On February 14, 2021, suspects attempted to rob a cell phone store in Byron Center, Michigan. They were not successful and fled the vehicle they were using. In the vehicle, police found a cell phone. On the cell phone, police discovered "multiple images" of the 1166 number. (*Id.*)

In July 2021, investigators conducted a proffer interview with an individual in custody on charges for larceny, burglary, receiving stolen property, and other offenses. (*Id.* at 15.) The individual identified Defendant from a photograph, saying that he referred to Defendant as "Arab." (*Id.* at 16.) The individual told investigators that he acted as a "middle-man" between Defendant and other members of the 1K Chicken Boys. (*Id.* at 16.) He would purchase stolen cell phones from the other gang members and then sell them to Defendant at meeting places in Michigan, Indiana, and Illinois. (*Id.*) He estimated selling over 100 stolen cell phones to Defendant. He said that Defendant would pay for the cell phones using bundles of "rubber-banded cash." (*Id.*)

That same month, investigators executed the warrant to search the iCloud account(s) associated with the 1166 number. There were three iCloud accounts associated with that number. (*Id.* at 17.) In one account, there was a screenshot of a request from March 2021 to start utility services at the apartment in Tinley Park, Illinois. (*Id.* at 17-18.) Also in the account were photographs, including one of Defendant holding several rubber-banded wads of cash while sitting in a car, and one of several packages of iPhones and Samsung earbuds next to a stack currency on a countertop. (*Id.* at 19.) The account also contained conversations regarding the sale and purchase of cell phones, as well advice from Defendant to members of 1K Chicken Boys about how to steal Apple items and how to avoid a high-speed police pursuit. (*Id.* at 20.)

Another iCloud account associated with the 1166 number used the email address tazboss79@gmail.com. In that account, there was a photograph of several boxes of Apple iPhones on a countertop, as well as two photographs of large amounts of currency. In one such photograph, $100 bills were laid out in a manner that spells "Taz" on what appears to be a Batman-themed bedsheet. (*Id.* at 21.) Defendant apparently calls himself "Taz" in text messages and in usernames for databases. (*Id.*)

Police also collected information confirming that Defendant resided at the Tinley Park apartment. After receiving a warrant for location information for the phone using the 1166 number, police discovered that the phone was within close proximity to the Tinley Park apartment building every night from May 3, 2021, to May 12, 2021. (*Id.* at 22.) While conducting surveillance of the apartment building, police saw Defendant depart the building on two occasions, once in May 2021 and once in October 2021. On both occasions, Defendant left the building and drove away in a 2014 Toyota Avalon that was parked nearby.

II. ANALYSIS

The Fourth Amendment protects individuals from "unreasonable searches and seizures." U.S. Const. amend. IV. It also provides that a warrant must have probable cause "supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.* "Probable cause 'is not a high bar.'" *Dist. of Columbia v. Wesby*, 583 U.S. 48, 57 (2018) (quoting *Kaley v. United States*, 571 U.S. 320, 338 (2014)). It "requires only a probability or substantial chance of criminal activity, not an actual showing of such activity[.]" *Id.* (quoting *Illinois v. Gates*, 462 U.S. 213, 243-44 n.13 (1983)). It exists where the "facts and circumstances" are "sufficient to warrant a prudent person . . . in believing . . . that the suspect has committed, is committing, or is about to commit an offense." *Michigan v. DeFillippo*, 443 U.S. 31, 37 (1979). It is a "practical and common-sensical standard" based on "the totality of the circumstances." *Florida v. Harris*, 568 U.S. 237, 244 (2013).

Thus, to obtain a proper search warrant, the officer "must submit an affidavit that 'indicate[s] a fair probability that evidence of a crime will be located on the premises of the proposed search.'" *United States v. Hines*, 885 F.3d 919, 923 (6th Cir. 2018) (quoting *United States v. Dyer*, 580 F.3d 386, 390 (6th Cir. 2009)). The warrant affidavit must also establish a "nexus between the place to be searched and the evidence sought." *United States v. Carpenter*, 360 F.3d 591, 594 (6th Cir. 2004) (en banc) (quoting *United States v. Van Shutters*, 163 F.3d 331, 336-37 (6th Cir. 1998)).

The Court examines the "four corners" of the affidavit "under the totality of the circumstances . . . with 'great deference toward' the determination of the judge who issued the search warrant." *United States v. Helton*, 35 F.4th 511, 518 (6th Cir. 2022) (quoting *United States v. Jackson*, 470 F.3d 299, 306 (6th Cir. 2006)).

III. ANALYSIS

A. Warrant for iCloud Account

Defendant apparently argues that the warrant affidavit to search the iCloud account associated with the 1166 number lacked probable cause because it relied on data obtained from another iPhone, seized in February 2021. However, that data included messages to and from the 1166 phone about the price of cell phones, as well as messages to the 1166 phone containing pictures of cell phones, at least one of which was confirmed as stolen from an AT&T store. Those messages occurred around the time of a robbery from an AT&T store in West Michigan. The affiant also relied on social media references to the 1166 number as a "plug," i.e., a source that would purchase stolen property. This information was sufficient to establish probable cause that the phone tied to the 1166 number had been used in furtherance of criminal activity, and that there was a fair probability that the phone had saved communications regarding the commission of a crime.

Defendant further argues that the affidavit did not establish a sufficient nexus to the iCloud account in particular because the affidavit did not describe the affiant's training and experience with cell phone technology or the examination of Apple devices that would permit the affiant to conclude that the device using the 1166 number was an Apple device with an iCloud account. The Court disagrees.

The affiant indicated that he has 22 years of experience conducting criminal investigations. (iCloud Warrant Aff. 1.) He also indicated that he had reviewed Apple's enforcement guidelines, which discuss the type of information that is stored by an Apple device on an iCloud account. (*Id.* at 26-29.) Those guidelines indicate that iCloud content may include "email, stored photos, documents, . . . [and] Messages[.]" (*Id.* at 28.) In addition, a device backup on an iCloud account may include "iMessage, Business Chat, SMS, and MMS messages[.]" (*Id.*) The use of

capitalization for the term "Messages" in the guidelines ostensibly means that term is referring to messages sent using iMessage, Apple's proprietary messaging software, as opposed to generic SMS and MMS text messages. Based on these guidelines, the affiant had a sufficient basis for believing that both Apple Messages and regular text messages sent to or from an iPhone may be stored in an iCloud account.

As support for the agent's conclusion that the 1166 number was an iPhone with an iCloud account, he asserted that the iCloud account for the iPhone seized by the police in February 2021[1] had stored messages from the 1166 phone, and that such storage typically only occurs "when both participants are using an iPhone and have the iMessages feature enabled." (iCloud Warrant Aff. 24.)

The Court finds that the support for the agent's conclusion is tenuous. The agent broadly referred to his "training and experience and investigation in this case" as the basis for his knowledge, but it is not entirely clear what experience he had with iPhones or iCloud accounts specifically, let alone experience that led him to believe that an iCloud account stores incoming messages only when the sender is using an iPhone. The Apple enforcement guidelines do not support the agent's assertion; they indicate that an iCloud account stores both iMessages and regular text messages. The guidelines do not distinguish messages received from iPhones from other messages. Indeed, it is counterintuitive to believe that an iPhone would, as a general matter, save texts and messages to iCloud only if they originated from another iPhone. Both the guidelines and common sense suggest that is not how it works.

[1] Defendant implies that the passage of time between February 2021 and June 2021, when police requested the warrant, rendered the information on the seized phone too stale to rely upon. Defendant does not expressly make or elaborate on this argument, however, so the Court will not address it.

Nevertheless, the warrant also referred to evidence of a Facetime conversation between the 1166 phone and another individual. (*Id.* at 5.) It is common knowledge that, at the time, the Facetime app was only available for use by iPhones. With this information, probable cause existed to believe that there was an iCloud account associated with the 1166 phone number and that this account would contain evidence of criminal activity.

Even if the foregoing facts were not sufficient for probable cause, the search easily satisfies the good faith exception in *United States v. Leon*, 468 U.S. 897 (1984). There, the Supreme Court held that evidence "'obtained in objectively reasonable reliance' on [a] 'subsequently invalidated search warrant' . . . should not be suppressed." *Helton*, 35 F.4th at 521 (quoting *Leon*, 468 U.S. at 922). The Court "identified four circumstances where an officer's reliance would not be objectively reasonable:"

> (1) the magistrate was "misled by information in the affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth;" (2) the magistrate "abandoned his judicial role" or neutrality; (3) the warrant was "so lacking in indicia of probable cause" as to render official belief in its existence unreasonable; or (4) the warrant was so "facially deficient" that it could not reasonably be presumed valid.

Id. (quoting *United States v. McClain*, 444 F.3d 556, 564-65 (6th Cir. 2005)).

The warrant here was not so facially deficient or lacking in probable cause as to render reliance upon it unreasonable. "An affidavit that is so lacking in indicia of probable cause that no reasonable officer would rely on the warrant has come to be known as a 'bare bones' affidavit." *United States v. White*, 874 F.3d 490, 496 (6th Cir. 2017) (quoting *United States v. Weaver*, 99 F.3d 1372, 1380 (6th Cir. 1996)). "To avoid the 'bare bones' label, the affidavit must contain 'more than suspicions, or conclusions'; it must provide 'some underlying factual circumstances regarding veracity, reliability, and basis of knowledge.'" *Helton*, 35 F.4th at 522 (quoting *United States v. Christian*, 925 F.3d 305, 312 (6th Cir. 2019)).

The warrant affidavit here was not a bare bones one. It relied on more than mere suspicions and conclusions to provide a link between criminal activity and an iCloud account associated with the 1166 number. To the extent Defendant challenges the factual basis for the conclusion that the phone with the 1166 number was an iPhone, the Facetime call is not the only basis for that conclusion. There is also evidence that the user of the 1166 phone was interested in purchasing iPhones specifically, as his price list referenced only iPhones. In addition, the evidence suggested that Defendant, who used the 1166 phone, gave stolen iPhones to his relatives. All these facts make it slightly more likely that the phone Defendant himself used, the 1166 phone, was an iPhone. These facts also distinguish the affidavit from a bare bones one. Thus, for all the foregoing reasons, the Court will not suppress evidence obtained from execution of that warrant.

B. Warrant for Defendant's Residence

Defendant argues that the warrant to search his apartment did not establish a nexus to his residence. He notes that there is no evidence that he met with robbery suspects at or near his apartment, and there is no evidence that he brought stolen items back to his residence.

In response, the Government cites *United States v. Sneed*, 385 F. App'x 551 (6th Cir. 2010), in which the Court of Appeals noted that "a nexus can be inferred based on the nature of the evidence sought and the type of offense that the defendant is suspected of having committed." *Id.* at 556. "One important inference that a reviewing court may consider is that 'it is reasonable to suppose that some criminals store evidence of their crimes in their homes, even though no criminal activity or contraband is observed there.'" *United States v. McCoy*, 905 F.3d 409, 417 (6th Cir. 2018) (quoting *United States v. Williams*, 544 F.3d 683, 686-87 (6th Cir. 2008)); *see United States v. Carney*, 675 F.3d 1007, 1013 (6th Cir. 2012) ("Just as a thief may be expected to have stolen goods in his home, or a drug dealer may be expected to have evidence of drug activity in his home, a purveyor of counterfeit bills of different denominations on different occasions may be expected

to have evidence of that activity in his home." (citations omitted)). For instance, "[e]vidence of a defendant's ongoing course of unlawful conduct may make it reasonable to conclude that he keeps evidence of his illegal scheme in his home." *Id.* Thus, in *United States v. Gunter*, 551 F.3d 472 (6th Cir. 2009), the defendant's sale of a large quantity of drugs and the "repeated nature" of his transactions made it reasonable to infer that evidence of illegal activity would be found at his residence, even though there was no evidence that he dealt drugs from his home. *Id.* at 481.

Similarly, the warrant affidavit in this case offered evidence suggesting that Defendant had been involved in many transactions to purchase stolen property. Several members of a gang suspected of involvement in burglaries in West Michigan referred to him as a "plug" for stolen phones. His vehicle traveled to Michigan on the same dates as five cell phone store robberies. There were also contacts between his phone and the phones of suspects involved in the robbery (or attempted robbery) of cell phone stores in Michigan. An individual in custody estimated that he sold over 100 stolen cell phones to Defendant. Defendant's phone received images of stolen cell phones after he sent a price list for iPhones. iCloud accounts associated with Defendant's phone contained images of stacks of cell phones and large amounts of currency, as well as communications related to the purchase of stolen cell phones. As in *Gunter*, the quantity and repeated nature of Defendant's receipt of stolen goods made it reasonable to infer that evidence of his illegal activity would be found in his residence. In addition, several of the photos found in the iCloud accounts appear to show stolen goods and currency on countertops and on a bedsheet, suggesting that the goods and currency were stored at a residence. These facts were sufficient to establish probable cause that a search of Defendant's residence would uncover evidence of criminal activity.

Alternatively, the good faith exception applies. Where there is insufficient basis for a nexus between the evidence sought and the location to be searched, the good faith exception may apply if there is a "minimally sufficient nexus." *Id.* at 522. "The minimally sufficient nexus standard is a 'less demanding showing than the "substantial basis" threshold required to prove the existence of probable cause.'" *Id.* (quoting *United States v. Fitzgerald*, 754 F. App'x 351, 362 (6th Cir. 2018)). Here, the extent of Defendant's apparent involvement in buying stolen cell phones and the photographs of cell phones and large amounts of currency provided the minimally sufficient nexus to give a reasonable officer a good faith basis for relying on the warrant.

IV. CONCLUSION

For all the foregoing reasons, the Court will deny Defendant's motion to suppress.

An order will enter that is consistent with this Opinion.

Dated: April 22, 2024

/s/ Hala Y. Jarbou
HALA Y. JARBOU
CHIEF UNITED STATES DISTRICT JUDGE